Confidential message electronic security with secret identification protocol code having verification process using polynomial formed from release polynomial/second polynomial and zero release where correspondence not found.

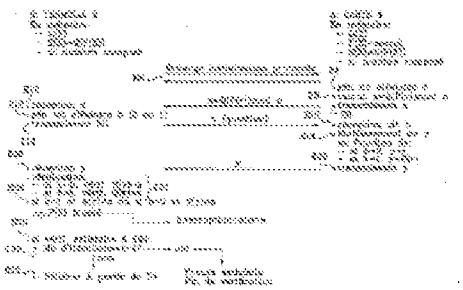
Publication number: FR2830147
Publication date: 2003-03-28
Inventor: JOYE MARC; NACCACHE DAVID; PORTE STEPHANIE
Applicant: GEMPLUS CARD INT (FR)
Classification:
- international: ***H04L9/32;*** **H04L9/32;** (IPC1-7): H04L9/32
- European: H04L9/32C
Application number: FR20010012275 20010924
Priority number(s): FR20010012275 20010924

Also published as:
WO03036865 (A1)

Report a data error here

Abstract of **FR2830147**

The process of verification of a confidential digital word has a first polynomial with the release mechanism transmitting digital words to the verifier. The verifier analyses the digital words using a second polynomial which is made up of the first and second polynomial only allowing information release when the two correspond.



(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 830 147**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 12275**

(51) Int Cl[7] : **H 04 L 9/32**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 24.09.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 28.03.03 Bulletin 03/13.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *GEMPLUS Société anonyme* — FR.

(72) **Inventeur(s) :** JOYE MARC, NACCACHE DAVID et PORTE STÉPHANIE.

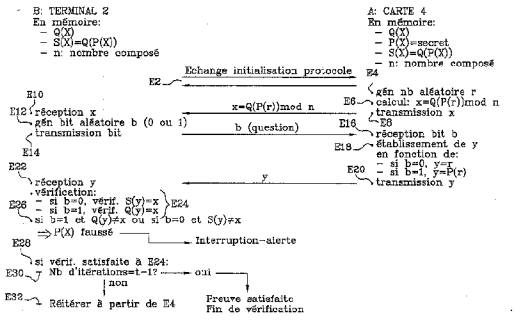
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BALLOT.

(54) PROCEDE ET DISPOSITIF DE LA VERIFICATION DE LA DETENTION D'UNE DONNEE CONFIDENTIELLE SANS COMMUNICATION DE CELLE-CI, SELON UN PROCESSUS DIT DE "A DIVULGATION NULLE".

(57) L'invention permet de procéder à une vérification, par un vérificateur (A, 2), de la détention d'au moins une donnée confidentielle (P (X); P_1 (X)... P_t (X)) par un détenteur présumé (B, 4), sans communication par ce dernier de la donnée confidentielle, conformément à un processus dit de " à divulgation nulle ".

A cette fin, il est prévu d'utiliser pour la donnée confidentielle au moins un premier polynôme (P (X)), le détenteur présumé (B, 4) transmettant au vérificateur (A, 2) des données (x, y) calculées en utilisant ce polynôme, la vérification étant établie sur la base d'une analyse de ces données mettant en oeuvre au moins un deuxième polynôme (Q (X)) et d'un polynôme composé Q (P (X)).



FR 2 830 147 - A1

2830147

Procédé et dispositif de la vérification de la détention d'une donnée confidentielle sans communication de celle-ci, selon un processus dit de "à divulgation nulle".

L'invention concerne la sécurisation électronique par code secret, par exemple pour des protocoles d'identification. Dans ce cadre, le code secret est typiquement attribué à une entité, désignée ci-après "détenteur", en tant que clé d'accès à une prestation d'un fournisseur. Cette clé est soumise à une vérification par un système de sécurisation lié au fournisseur, qui conditionne l'accès à la prestation. Le processus de demande d'autorisation s'effectue par échange électronique entre le détenteur présumé et le fournisseur.

La figure 1 illustre très schématiquement le cas général d'un ensemble composé d'une part d'un système de vérification (vérificateur) 2 et d'autre part d'un détenteur présumé 4. Le système 2 et le détenteur présumé communiquent sur une liaison 6 qui peut être locale ou distante (par réseau), filaire, radioélectrique, infrarouge, etc. Dans l'exemple, le détenteur présumé 4 se trouve être matérialisé par une carte à puce, le système de vérification 2 étant un terminal avec lecteur de carte. Le code secret (désigné par le terme "secret" dans ce qui suit) est alors contenu au sein d'une mémoire de la carte 2. La vérification de la validité du secret nécessite un échange de messages sur la liaison 6 selon un protocole préétabli. La vérification peut conditionner l'accès à un service (téléphonique, de réception de télévision à péage, de transaction bancaire ou commerciale), ou à contrôler l'accès à un site, la transmission d'un dossier médical, l'identification d'une personne, etc.

Dans une mise en œuvre classique, le protocole prévoit la transmission du secret vers le terminal, éventuellement sous forme cryptée pour éviter des attaques durant l'échange.

Cependant, il existe aussi des protocoles dits de "à divulgation nulle" (de l'anglais "zéro knowledge"), basés sur le fait qu'il est mathématiquement possible à un détenteur présumé de prouver qu'il possède effectivement un secret valable sans pour autant le communiquer au système de vérification. Il s'agit de protocoles de preuve de détection de secret sans divulgation ou de protocoles à divulgation nulle. Les protocoles Fiat-Shamir, Guillou-Quisquatter, "syndrome decoding", "permuted kernels problem", "constrained linear equations", etc. sont des exemples de tels protocoles de à divulgation nulle. Le principe repose sur un échange de questions et de réponses, provenant respectivement du système de sécurisation 2 et du détenteur présumé 4. Le protocole d'identification est de nature asymétrique, en ce sens qu'il fait appel à des clés privées et publiques, la clé privée constituant le secret détenu au niveau du détenteur présumé. Puisque le secret n'est jamais révélé durant le protocole, il n'y a pas de risque qu'il soit approprié par un détenteur présumé mal intentionné, ou une personne interceptant les messages échangés en vue de pouvoir se présenter comme le détenteur agréé du secret.

Si ces protocoles permettent une sélection de paramétrage, leur conception demeure relativement figée. Ceci est notamment le cas avec le protocole de Fiat et Shamir.

Ainsi, un objet de l'invention est de prévoir une sécurisation par vérification basée sur un nouveau protocole de à divulgation nulle, permettant de

nombreuses possibilités de mise en oeuvre selon les applications envisagées.

Plus particulièrement, l'invention propose, selon un premier objet, un procédé de vérification, par un vérificateur, de la détention d'au moins une donnée confidentielle P(X); $P_1(X)$... $P_t(X)$ par un détenteur présumé, sans communication par ce dernier de la donnée confidentielle, conformément à un processus dit de "à divulgation nulle",

caractérisé en ce que l'on utilise pour la donnée confidentielle au moins un premier polynôme P(X), le détenteur présumé transmettant au vérificateur des données calculées en utilisant ce polynôme, la vérification étant établie sur la base d'une analyse de ces données mettant en œuvre au moins un deuxième polynôme Q(X) et d'un polynôme composé S(X) = Q(P(X)), celui-ci étant composé du premier polynôme P(X) et du deuxième polynôme Q(X).

Avantageusement, à partir :

- du premier polynôme, soit P(X) d'une variable X, et
- du deuxième polynôme, soit Q(X) de la variable X,

on définit un troisième polynôme composé S(X) = Q(P(X)),

et on met en œuvre au moins une séquence comprenant les étapes de :

a) transmission, du détenteur présumé au vérificateur, d'une première donnée (x) obtenue à partir du troisième polynôme S(X) pour le cas de la variable X = r, soit Q(P(r)), où r est un nombre choisi arbitrairement par le détenteur présumé ;

b) transmission en réponse, du vérificateur au détenteur présumé, d'une valeur d'invitation de preuve (b),

c) transmission, du détenteur présumé au vérificateur, d'une deuxième donnée (y) calculée selon $y = r$ si la valeur d'invitation de preuve b correspond à une première valeur et selon $y = P(r)$ si la valeur d'invitation de preuve correspond à une seconde valeur, et

d) vérification, par le vérificateur, que la condition $S(y) = x$ est satisfaite si la valeur d'invitation de preuve correspond à la première valeur, et que la condition $Q(y) = x$ est satisfaite si la valeur d'invitation de preuve correspond à la seconde valeur, une vérification positive à l'étape d) accroissant le degré de confiance en la détention effective de la donnée secrète $P(X)$ par le détenteur présumé.

Le procédé peut être mis en œuvre pour une vérification portant sur une pluralité t de données confidentielles indépendantes, chacune définie par un premier polynôme respectif, où, à partir :

- des premiers polynômes respectifs, soit $P_1(X)$, $P_2(X)$, $P_3(X)$,..., $P_t(X)$ d'une variable X, et
- du deuxième polynôme, soit $Q(X)$ de la variable X,

on définit un troisième ensemble de fonctions $S_i(X)$ pour $i = 0$ à t, soit : $S_0 = Q(X)$, $S_1(X) = Q(P_1(X))$, $S_2(X) = Q(P_1(P_2(X)))$, $S_3(X) = Q(P_1(P_2(P_3(X))))$, ...$S_t(X) = Q(P_1(P_2(P_3(\ldots P_t(X)))))$,

et on met en œuvre au moins une séquence comprenant les étapes de :

- i) transmission, du détenteur présumé au vérificateur, d'une première donnée (x) obtenue à partir de la fonction $S_t(X)$ pour le cas de la variable $X = r$, soit $x = Q(P_1(P_2(P_3(\ldots P_t(r)))))$, où r est une valeur aléatoire générée au niveau du détenteur présumé;

- ii) transmission, du vérificateur au détenteur, présumé d'une désignation arbitraire ou pas d'une ou plusieurs fonction(s) parmi un ensemble de fonctions E_i de variable X, soit :

fonction E_0 : P1(P2(P3(…(Pt(X))…))),
fonction E_1 : P2(P3(…Pt(X)…)),
fonction E_2 : P3(…Pt(X)…)
…
fonction E_t : X ;

- iii) transmission, du détenteur présumé au vérificateur, d'une deuxième donnée (yi) calculée selon la fonction désignée E_i à l'étape précédente pour le cas de la variable X = r ou d'un nombre correspondant de valeurs yi, chacune étant obtenue à partir d'une fonction désignée respective ; et

- iv) vérification, par le vérificateur, que la condition $S_i(y_i)= x$ est satisfaite pour chacune des valeurs correspondantes.

De préférence, on répète la séquence d'étapes i) à iv) au moins une fois, une fonction E_i étant désignée arbitrairement à chaque répétition de séquence.

Avantageusement, tous les polynômes (P(X), Q(X), S(X); $S_i(X)$, $E_i(X)$) sont définis modulo n, où n est un nombre composé difficilement factorisable.

La donnée confidentielle peut être constituée d'un polynôme P(X) d'ordre 2 (deux) ou supérieur.

Le deuxième polynôme (Q(X)) peut être un polynôme d'ordre 2 (deux) ou supérieur.

Selon un deuxième aspect, l'invention concerne un dispositif de vérification spécifiquement adapté pour réaliser le procédé selon le premier objet.

Selon un troisième aspect, l'invention concerne un dispositif détenteur d'au moins une donnée confidentielle spécifiquement adapté pour réaliser le

procédé selon le premier aspect, ce dispositif pouvant être une carte à puce.

L'invention et les avantages qui en découlent seront mieux compris par la description qui suit des modes de réalisation préférés, donnés purement à titre d'exemple non-limitatif, par référence aux dessins en annexe, dans lesquels :

- la figure 1, déjà décrite, est un schéma général simplifié d'un ensemble constitué d'un système de sécurisation et d'un détenteur présumé, avec échange de données de vérification de secret ;

- la figure 2 est un organigramme du déroulement d'un procédé de vérification entre un terminal et une carte selon un protocole de à divulgation nulle conforme à un premier mode de réalisation de l'invention ; et

- la figure 3 est un organigramme du déroulement d'un procédé de vérification entre un terminal et une carte selon un protocole de à divulgation nulle conforme à un second mode de réalisation de l'invention.

La sécurité du protocole de vérification à divulgation nulle selon l'invention repose sur le problème suivant. Soient deux polynômes P(X) et Q(X), on peut facilement calculer le polynôme composé S(X) = Q(P(X)). Mais, étant donnés Q(X) et S(X), il est difficile trouver P(X. Dans ce qui suit, tous les calculs sont réalisés en arithmétique modulo n, où n est un nombre composé. A titre d'exemple, le nombre n peut être le produit de deux nombres premiers p et q, soit n=p.q. Le secret, dont la connaissance est à prouver par le détenteur, est le polynôme P(X).

Dans ce qui suit, on désigne par A le détenteur du secret P(X) (détenteur présumé), et par B le vérificateur du fait que A connaisse effectivement le

secret P(X). "A" peut être une carte à puce 4 ou analogue, et "B" le système de sécurisation 2, pour reprendre l'exemple de la figure 1. Ainsi, conformément au protocole "à divulgation nulle", A doit prouver à B qu'il détient le secret P(X) sans le lui révéler.

La figure 2 illustre un exemple du déroulement d'un protocole de vérification "à divulgation nulle" conforme à l'invention, appliqué à l'ensemble de la figure 1.

Au préalable, le détenteur présumé A du secret P(X), soit la carte 4, contient dans sa mémoire les paramètres suivants :

- un polynôme P(X), qui constitue un paramètre privé, soit le secret. On note que le paramètre privé qui constitue le secret est le polynôme P(X) qui est le polynôme difficile à trouver selon le problème énoncé ci-dessus,

- une fonction polynomiale S(X) définie par : S(X) = Q(P(X)), et

- un module n difficilement factorisable, par exemple de type RSA.

La fonction S(X) s'obtient directement par calcul à partir des polynômes P(X) et Q(X). A titre illustratif, donné ici seulement pour comprendre ce mode de calcul, si $Q(X) = aX^2 + bX + c$ et $P(X) = u_1X + u_0$, alors :

$$\begin{aligned} S(X) &= a(u_1X + u_0)^2 + b(u_1X + u_0) + c \\ &= a(u_1^2X^2 + u_0^2 + 2u_1u_0X) + u_1bX + u_0b + c \\ &= au_1^2X^2 + (2au_1u_0 + u_1b)X + au_0^2 + u_0b + c \\ &:= s_2X^2 + s_1X + s_0 \end{aligned}$$

Les coefficients des polynômes a, b, c, u1 et u0, ainsi que s_2, s_1 et s_0 sont des valeurs connues par la carte. Cependant, pour réduire le nombre d'arguments à

stocker, la carte peut ne pas contenir les paramètres relatifs à Q(X), c'est-à-dire a, b et c.

Q(X) et P(X) sont des polynômes en X de degré p et q. Ils sont réduits modulo n, c'est-à-dire que leurs coefficients sont réduits modulo n. A titre d'exemple,

pour $P(X) = \Sigma_{i=0 \text{ à } p} a_i X^i = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \ldots + a_p X^p$,

$P(X) \bmod n = (\Sigma\ i=0 \text{ à } p\ a_i X^i) \bmod n$

$= \Sigma\ i=0 \text{ à } p\ (a_i \bmod n) X^i$.

De son côté, le système B de vérification (vérificateur) de la connaissance du secret, soit le terminal 2, contient dans sa mémoire les mêmes paramètres que ceux stockés par la carte, hormis le secret P(X), à savoir : Q(X), S(X) = Q(P(X)) et n.

En début de protocole, il s'opère un échange de signaux entre le terminal 2 et la carte 4 pour établir l'initialisation du processus (étape E2). Durant cette phase, une série de routines est installée pour fixer les conditions de vérification.

Le processus de vérification "à divulgation nulle" débute alors par le tirage d'un nombre aléatoire r au niveau de la carte 4 (étape E4). Ce nombre r est produit par des algorithmes quelconques. A partir de ce nombre r, la carte calcule une valeur x donnée par la fonction S(X) mod n, pour X = r, soit x = Q(P(r)) mod n. La carte envoie cette valeur de x au terminal 2 (étape E8), où elle y est réceptionnée (étape E10).

Ensuite, le terminal produit un bit b dit d'interrogation ou d'invitation de preuve (étape E12). Dans l'exemple, les probabilités de b = 1 et b = 0 sont égales. Ce bit b est transmis à la carte (étape E14), où elle constitue la partie "question" selon l'aspect question-réponse du protocole à divulgation nulle.

La carte réceptionne le bit b (étape E16) et produit en réponse une valeur y en fonction de la valeur de ce bit, comme suit (étape E18):

- si b = 0, y = r ;
- si b = 1, y = P(r), c'est-à-dire la valeur rendue par le polynôme secret P(X) pour X = r.

Ensuite, la carte 4 envoie la valeur y au terminal 2 (étape E20), où elle est y réceptionnée (étape E22). La valeur de b conditionne la nature de la vérification effectuée par le terminal 2, comme suit (étape E24) :

- si b = 0, le terminal vérifie que S(y) = Q(P(y)) = x ;
- si b = 1, le terminal vérifie que Q(y) = x. Les étapes précédantes impliquées dans les trois séries d'échanges, en commençant par l'étape E4 de génération d'un nombre aléatoire, doivent être itérées plusieurs fois afin de garantir un degré de confiance suffisant, chaque nouvelle itération permettant de se rapprocher du niveau de confiance souhaité.

En revanche, il suffit qu'une seule instance de la vérification à l'étape E24 soit non satisfaite pour permettre de constater que la carte 2 ne détient pas le secret P(X). Dans le cas d'un tel constat, le terminal initie une routine d'interruption de la procédure de vérification pour cause d'échec, et déclenche une alerte adaptée aux circonstances (étape E26).

Lorsque la condition à vérifier satisfaite à l'étape E24, la procédure entame une itération du processus à partir de l'étape E4 afin de pouvoir renforcer le degré de confiance.

Le protocole de vérification conforme à l'invention est très sûr, permettant d'obtenir des degrés de confiance C arbitrairement proches de 1. En effet, à supposer que les polynômes P(X) et Q(X) soient

bien choisis, pour $S(X) = Q(P(X))$ donné modulo n, le problème de retrouver $P(X)$ à partir de $S(X)$ et de $Q(X)$ est supposé difficile.

Il n'existe pas de règles générales de sélection des polynômes $P(X)$ et $Q(X)$. On choisira de manière empirique des polynômes qui soient suffisamment complexes pour ne pas permettre de déduire aisément la valeur du secret. Avantageusement, au moins l'un de ces polynômes doit être de degré 2 ou supérieur.

L'utilisation du modulus n pour exprimer x implique que tous les coefficients des polynômes doivent être réduits par ce modulus, ce qui renforce la difficulté du problème de trouver $P(X)$ à partir de $Q(P(X))$ et de $S(X)$.

A titre indicatif, d'excellents résultats sont obtenus en termes de sécurité et de consommation de ressources avec le choix suivant de polynômes :

$P(X) = u_2X^2 + u_1X + u_0$, et $Q(X) = aX^2 + bX + c$

$S(X) = c_4X^4 + C_3X^3 + c_2X^2 + c_1X + c_0$, où les coefficients a, b, c et c_4, c_3, c_2, c_1 et c_0 sont connus.

Le problème de trouver $P(X)$ à partir de $Q(X)$ et de $S(X)$ est alors équivalent à déterminer une racine carrée en modulo n.

Il sera maintenant décrit une généralisation du mode de réalisation selon laquelle on utilise un nombre arbitraire t de clés privées. Cette disposition permet notamment de réduire le nombre d'échanges entre le fournisseur (terminal 2) et le détenteur présumé (carte 4), notamment en s'affranchissant des itérations précitées, ou tout au moins en réduisant leur nombre. L'approche consiste à utiliser dans le processus de vérification plusieurs clés publiques et un nombre correspondant de clés privées, stockées respectivement au niveau du terminal 2 et de la carte 4. Cette approche s'inscrit dans un cadre général de mise en

oeuvre, avec utilisation d'un nombre t de clés privés $P_1(X)$, $P_2(X)$, $P_3(X)$, ..., $P_t(X)$ associées à t clés publiques respectives, celles-ci étant :

$S_1(X) = Q(P_1(X))$,

$S_2(X) = Q(P_1(P_2(X)))$,

$S_3(X) = Q(P_1(P_2(P_3(X))))$

...

$S_t(X) = Q(P_1(P_2(P_3(\ldots P_t(X)))))$.

Dans ce qui suit, tous les polynômes sont réduits modulo n, comme dans le cas précédent ; ce fait ne sera pas répété systématiquement par souci de concision.

Lors d'une vérification, le terminal 2 et la carte 4 entament un processus d'échange de données préliminaires pour l'initialisation du protocole (étape E2), à l'instar du mode de réalisation de la figure 2.

Ensuite, la carte 4 produit un nombre aléatoire r (étape E4), calcule à partir de ce nombre une valeur $x = Q(P_1(P_2(P_3(\ldots(P_t(r))))\ldots)$ (étape E30), et la transmet au terminal 2 (étape E32).

En réponse, le terminal produit un nombre aléatoire b dans un domaine d'équiprobabilité 0 à t compris (étape E34) et le transmet à la carte 4 (étape E36).

En fonction du nombre b, la carte calcule la valeur y_i, sélectionnée selon la valeur de b, (étape E38).

Plus particulièrement, la valeur y_i est déterminée comme suit :

si $b = 0$, $y_0 = P_1(P_2(P_3(\ldots(P_t(r)\ldots))))$,

si $b = 1$, $y_1 = P_2(P_3(\ldots(P_t(r)\ldots))$,

si $b = 2$, $y_2 = P_3(\ldots(P_t(r)\ldots)$,

...

si $b = t$, $y = r$.

On remarque que les réponses y_i de la carte en fonction de la valeur de b envoyé par le terminal sont basées sur les clés publiques

$S_1(X)$, $S_2(X)$, $S_3(X)$, $S4(X)$, ..., $St(X)$

La valeur y_i requise ainsi calculée est transmise au terminal (étape E40).

A la réception de cette valeur y_i, le terminal procède à une vérification en fonction de la valeur de b (étape E42) :

si b = 0, vérification de la condition $Q(y_0) = x$

si b = 1, vérification de la condition $S_1(y_1) = x$

si b = 2, vérification de la condition $S_2(y_2) = x$

... ...

... ...

si b = t, vérification de la condition $S_t(y_t) = x$

Si la condition à vérifier à l'étape E42 est satisfaite, on peut supposer (étape E44) avec un certain degré de confiance que le détenteur présumé a prouvé qu'il détient le secret. Dans le cas contraire, on suppose que la preuve demandée n'a pas été fournie pour des raisons suspectes, et la communication avec la carte 4 est interrompue, éventuellement accompagné d'une procédure d'alerte.

Si le nombre t de clés utilisées dans la procédure ne permet pas d'obtenir un degré de confiance suffisant, il est bien entendu envisageable de réaliser une ou plusieurs itérations à partir de l'étape E4.

Selon une variante du mode de réalisation de la figure 3, le terminal 2 transmet à l'étape E36 non pas une, mais plusieurs valeurs de b, chacune choisie de manière aléatoire.

La carte 4 calcule alors à l'étape E38 une valeur y_i en fonction de chacune des valeurs de b reçues, sur les mêmes bases que pour le calcul de y_i décrit par référence à la figure 3, et les transmet au terminal.

Le terminal analyse chacune des valeurs y_i ainsi reçues pour déterminer si elles satisfont les conditions énoncées supra dans le cadre de l'étape E42.

On comprendra que cette variante permet à la carte de détenir plusieurs secrets. Le terminal peut alors vérifier la connaissance de ces secrets en une seule série d'opérations, par exemple, lors d'une vérification simultanée de plusieurs mots de passe ou de codes d'authentification.

L'invention n'est pas limitée aux cartes ou à des dispositifs portatifs, trouvant application dans tout système de communication faisant appel à une identification confidentiel : vérification de mot passe entre un utilisateur et son ordinateur, son véhicule, matériel professionnel, téléphone mobile, ou autre équipement personnalisé, etc.

REVENDICATIONS

1. Procédé de vérification, par un vérificateur (B,2), de la détention d'au moins une donnée confidentielle (P(X); $P_1(X)$... $P_t(X)$) par un détenteur présumé (A,4)), sans communication par ce dernier de la donnée confidentielle, conformément à un processus dit de "à divulgation nulle",

caractérisé en ce que l'on utilise pour la donnée confidentielle au moins un premier polynôme (P(X)), le détenteur présumé (A,4)) transmettant au vérificateur (B,2) des données (x, y; y_i) calculées en utilisant ce polynôme, la vérification étant établie sur la base d'une analyse de ces données mettant en œuvre au moins un deuxième polynôme Q(X) et d'un polynôme composé S(X) = Q(P(X)), celui-ci étant composé du premier polynôme P(X) et du deuxième polynôme Q(X).

2. Procédé selon la revendication 1, caractérisé en ce que, à partir :

- dudit premier polynôme, soit P(X) d'une variable X, et
- dudit deuxième polynôme, soit Q(X) de la variable X,

on définit un troisième polynôme composé S(X) = Q(P(X)),

et en ce qu'il met en œuvre au moins une séquence comprenant les étapes de :

a) transmission, du détenteur présumé (A,4) au vérificateur (B,2), d'une première donnée (x) obtenue à partir dudit troisième polynôme S(X) pour le cas de la variable X = r, soit Q(P(r)), où r est un nombre choisi arbitrairement par le détenteur présumé ;

b) transmission en réponse, du vérificateur (B,2) au détenteur présumé, d'une valeur d'invitation de preuve (b),

c) transmission, du détenteur présumé au vérificateur, d'une deuxième donnée (y) calculée selon $y = r$ si la valeur d'invitation de preuve b correspond à une première valeur et selon $y = P(r)$ si la valeur d'invitation de preuve correspond à une seconde valeur, et

d) vérification, par le vérificateur, que la condition $S(y) = x$ est satisfaite si la valeur d'invitation de preuve correspond à la première valeur, et que la condition $Q(y) = x$ est satisfaite si la valeur d'invitation de preuve correspond à la seconde valeur, une vérification positive à l'étape d) accroissant le degré de confiance en la détention effective de la donnée secrète $P(X)$ par le détenteur présumé (A,4).

3. Procédé selon la revendication 1, caractérisé en ce qu'il est mis en œuvre pour une vérification portant sur une pluralité t de données confidentielles indépendantes, chacune définie par un premier polynôme respectif, caractérisé en ce que, à partir :

- desdits premiers polynômes respectifs, soit $P_1(X)$, $P_2(X)$, $P_3(X)$,..., $P_t(X)$ d'une variable X, et
- dudit deuxième polynôme, soit $Q(X)$ de la variable X,

on définit un troisième ensemble de fonctions $S_i(X)$ pour $i = 0$ à t, soit : $S_0 = Q(X)$, $S_1(X) = Q(P_1(X))$, $S_2(X) = Q(P_1(P_2(X)))$, $S_3(X) = Q(P_1(P_2(P_3(X))))$, ...$S_t(X) = Q(P_1(P_2(P_3(\ldots P_t(X)))))$,

et ce que l'on met en œuvre au moins une séquence comprenant les étapes de :

- i) transmission, du détenteur présumé (A,4) au vérificateur (B,2), d'une première donnée (x) obtenue à partir de la fonction $S_t(X)$ pour le cas de la variable $X = r$, soit $x = Q(P_1(P_2(P_3(\ldots P_t(r)))))$, où r est une valeur aléatoire générée au niveau du détenteur présumé (B,4) ;

- ii) transmission, du vérificateur au détenteur, présumé d'une désignation arbitraire ou pas d'une ou plusieurs fonction(s) parmi un ensemble de fonctions E_i de variable X, soit :

fonction E_0 : P1(P2(P3(…(Pt(X))…)),
fonction E_1 : P2(P3(…Pt(X)…)),
fonction E_2 : P3(…Pt(X)…)
…
fonction E_t : X ;

- iii) transmission, du détenteur présumé au vérificateur, d'une deuxième donnée (yi) calculée selon la fonction désignée E_i à l'étape précédante pour le cas de la variable X = r ou d'un nombre correspondant de valeurs yi, chacune étant obtenue à partir d'une fonction désignée respective ; et

- iv) vérification, par le vérificateur, que la condition $S_i(y_i) = x$ est satisfaite pour chacune desdites valeurs correspondantes.

4. Procédé selon la revendication 3, caractérisé en ce que ladite séquence d'étapes i) à iv) est répétée au moins une fois, une fonction E_i étant désignée arbitrairement à chaque répétition de séquence.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que tous les polynômes (P(X), Q(X), S(X); $S_i(X)$, $E_i(X)$) sont définis

modulo n, où n est un nombre composé difficilement factorisable.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que la donnée confidentielle est constituée d'un polynôme P(X) d'ordre 2 (deux) ou supérieur.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que ledit deuxième polynôme (Q(X)) et un polynôme d'ordre 2 (deux) ou supérieur.

8. Dispositif de vérification (B,2) permettant de vérifier la détention d'au moins une donnée confidentielle (P(X), $P_1(X)$, ..., $P_t(X)$ par un détenteur présumé (A,4), sans communication par ce dernier de la donnée confidentielle, conformément à un processus dit de « divulgation nulle »

caractérisé en ce qu'il est prévu pour réaliser le procédé de vérification selon l'une quelconque des revendications 1 à 7, le dispositif (B,2) comportant :

- des moyens de réception desdites données (x, y, y_i) calculées par le détenteur présumé (A,4),
- des moyens de stockage dudit polynôme composé S(X) = Q(P(X)), et
- des moyens d'analyse desdites données reçues mettant en oeuvre ledit polynôme composé (S(X) = Q(P(X)).

9. Dispositif (A,4) détenteur d'au moins une donnée confidentielle sujette à une vérification par un vérificateur (B,2) sans qu'elle soit communiquée à ce dernier, conformément à un processus dit de « divulgation nulle »,

caractérisé en ce qu'il est prévu pour réaliser le procédé de vérification selon l'une quelconque des revendications 1 à 7, le dispositif (A,4) comportant :

- des moyens de stockage dudit premier polynôme P(X), et
- des moyens de calcul mettant en oeuvre ledit premier polynôme pour produire lesdites données calculées (x, y, y_i), et
- des moyens de transmission desdites données calculées au vérificateur (B,2).

10. Dispositif selon la revendication 9, caractérisé en ce qu'il s'agit d'une carte à puce (4).

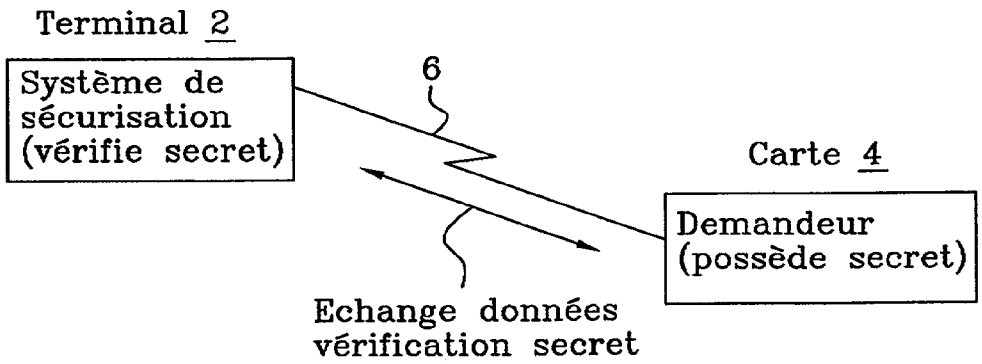

Terminal 2
Système de sécurisation (vérifie secret)
6
Carte 4
Demandeur (possède secret)
Echange données vérification secret

Fig. 1

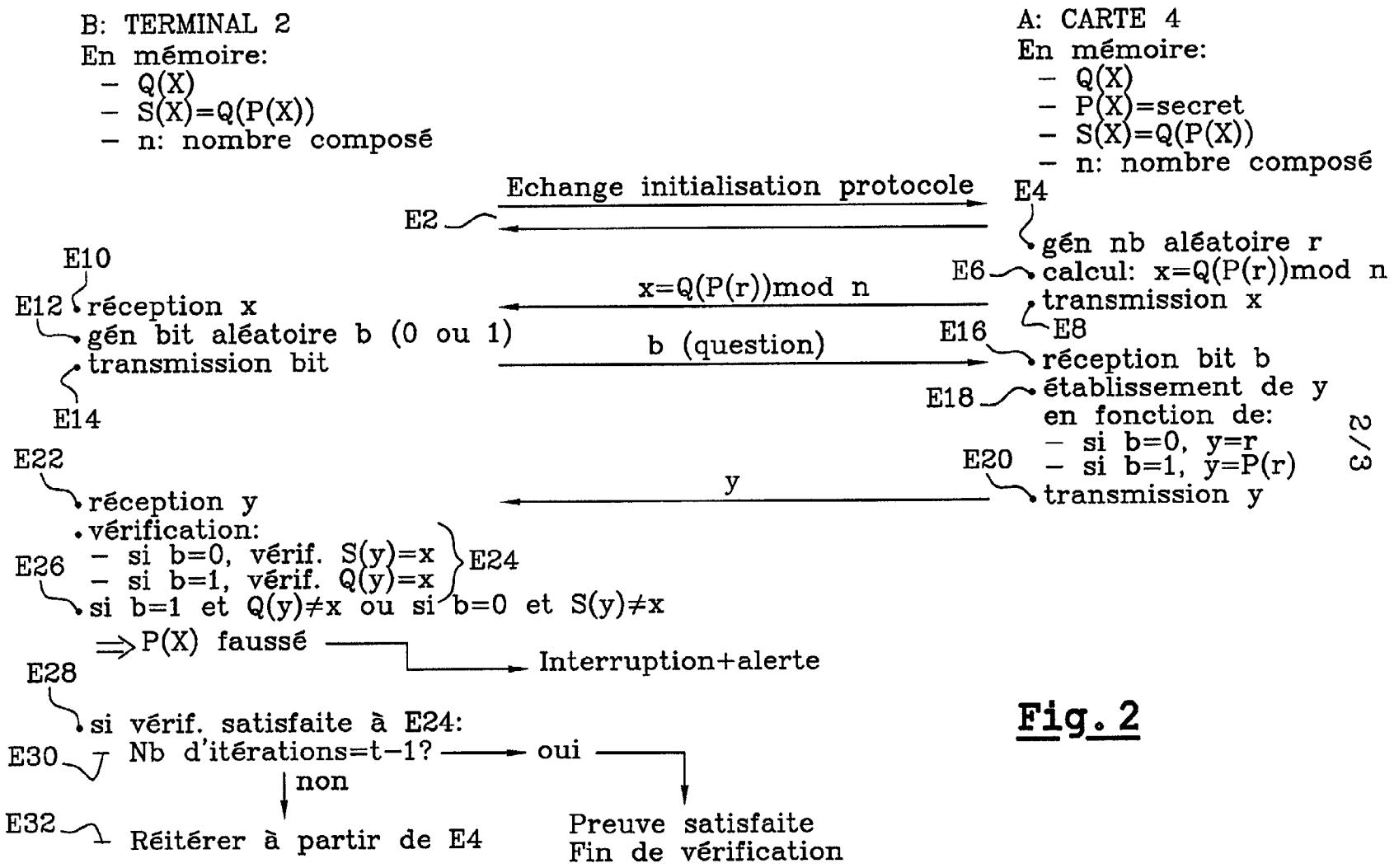


Fig. 2

2830147

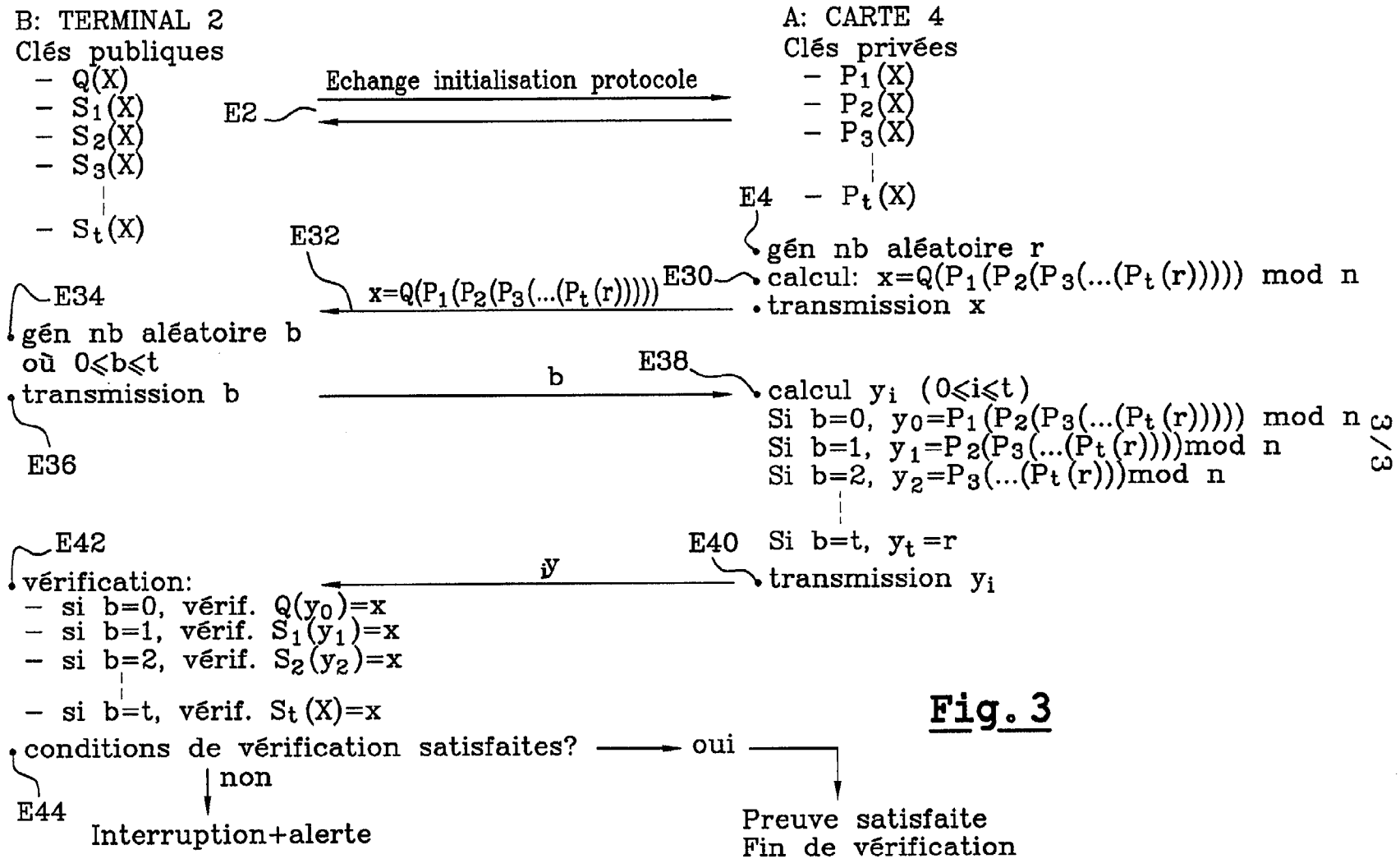


Fig. 3

2830147

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2830147

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national
FA 615075
FR 0112275

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
A	FIAT A ET AL: "HOW TO PROVE YOURSELF: PRACTICAL SOLUTIONS TO IDENTIFICATION AND SIGNATURE PROBLEMS" ADVANCES IN CRYPTOLOGY. SANTA BARBARA, AUG. 11 - 15, 1986, PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 6, 1986, pages 186-194, XP000090668 * page 187, ligne 3 - page 188, ligne 35 *	1,8,9	H04L9/32
A	NAOR M, PINKAS B: "Oblivious transfer and polynomial evaluation" PROCEEDINGS OF STOC 99: 31ST ANNUAL SYMPOSIUM ON THEORY OF COMPUTING , mai 1999 (1999-05), pages 245-254, XP002206822 * page 250, colonne de gauche, ligne 31 - page 251, colonne de gauche, ligne 32 *	1,8,9	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

H04L

Date d'achèvement de la recherche: 19 juillet 2002

Examinateur: Dujardin, C

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)